

VERIFICATION OF TRANSLATION

I, Tomoko HARA, translator of 6th floor, Yodogawa 5-Bankan, 3-2-1 Toyosaki, Kita-Ku, Osaka, Japan, hereby declare that I am conversant with the English and Japanese languages and am a competent translator thereof. I further declare that to the best of my knowledge and belief the following is a true and correct translation made by me of a Notification of Reasons for Refusal issued for Japanese Patent Application No. 2006-519466 by the Japanese Patent Office on October 23, 2007.

Date: February 21, 2008

原 明子

Tomoko HARA

## Notification of Reasons for Refusal

October 23, 2007

Application Number: Japanese Patent Application No. 2006-519466

Drafting Date: October 19, 2007

Patent Office Examiner: Nobuyuki Ishida 9469 5S00

Representative: Shiro Nakajima

Applied Article: the body of Article 29; Article 29, paragraph 2; Article 36

The above-identified application is rejected for the reason(s) given below. The applicant may respond to this office action within 60 days of the mailing date of this Office Action.

### Bases for Rejection

1. As to the invention of the following claims of the present application, one of ordinary skill in the art could have readily realized it before the time of the invention, based on inventions described in the following publications which were distributed in Japan or the other countries or inventions publicly available through electric communication lines before the date of the application of the invention. As a result, the invention is not patentable under the provision of Japanese Patent Act Article 29, paragraph 2.

2. The invention of the flowing claims of the present application is not patentable since it does not meet the requirements stated in the body of Article 29, paragraph 1 for the following reasons.

3. As to the present application, the claims do not meet the requirements stated in Article 36(6)(2) for the following reasons.

### Details

(regarding cited reference(s), see the list of the cited references)

- Basis 1

- Claim 11
- Reference 1-3

[Remarks]

Reference 1 (see Claims; page 2, left lower column, line 12 – page 3, right upper column, line 9), Reference 2 (FIGs. 1-8), and Reference 3 (FIGs. 1-4, 11 and 12) describe an information recording method for generating a plurality of record digest values (individual MACs, compressed text H(i), digests) generated from a plurality of data blocks (blocks, divided messages, digital documents) constituting a digital work (messages, files, a plurality of digital documents) and record signature data (global MAC, verification data H, integrated digest) generated based on some or all of the plurality of record digest values.

- Basis 2

[Remarks]

(A) The invention of Claim 11 is only characterized by (i) a plurality of record digest values generated from a plurality of data blocks and (ii) record signature data generated based on some or all of the plurality of record digest values, both of which are to be recorded on a recording medium. This is merely presentation of information and cannot be considered as technical means utilizing natural laws, and accordingly does not meet the requirements stated in the body of Article 29, paragraph 1.

(B) The invention stated in Claims does not specify hardware resources of the data processing apparatus to be used to perform information processing in the following respects. Accordingly, it does not use technical means utilizing natural laws, and thus does not meet the requirements stated in the body of Article 29, paragraph 1.

(1) The description of Claim 13 “a using step of using the digital work recorded on the recording medium; a selecting step of randomly selecting a predetermined number of data blocks from the plurality of data blocks, ....., and a

use controlling step of stopping the use of the digital work when the result of the verification is judged not valid” does not specify which hardware resources of the data processing apparatus to be used to 1) use the digital work recorded on the recording medium; 2) select the predetermined number of data blocks; 3) calculate a calculation digest values with respect to each of the selected data blocks; 4) read remaining record digest values, each of which corresponds to one of the unselected data blocks; and 5) verify whether the digital work recorded on the recording medium is valid. Accordingly, it is not considered that the invention is realized concretely using hardware resources.

(Consider, for example, describing clearly the use of hardware resources of the data processing apparatus, such as a using unit, a selecting unit, a calculating unit, a reading unit, a signature verifying unit and a use controlling unit. The same goes for (2) and the subsequent sections.)

(2) The description of Claim 14 “a using step of using the digital work recorded on the recording medium; a selecting step of randomly selecting a predetermined number of data blocks from the plurality of data blocks, ....., and a use controlling step of stopping the use of the digital work when the result of the verification is judged not valid” does not specify which hardware resources of the data processing apparatus to be used to 1) use the digital work recorded on the recording medium; 2) select the predetermined number of data blocks; 3) calculate a calculation digest values with respect to each of the selected data blocks; 4) read remaining record digest values, each of which corresponds to one of the unselected data blocks; and 5) verify whether the digital work recorded on the recording medium is valid. Accordingly, it is not considered that the invention is realized concretely using hardware resources.

• Basis 3

[Remarks]

Each component or the relationship between each component of the invention described in Claims is not clear in the following respects.

(1) Regarding the description “a using unit (using step) operable to use the digital work recorded on the recording medium” of Claims 1, 13 and 14, it is not clear what “to use the digital work” concretely means.

(2) Regarding the description “a signature verifying unit operable to verify whether the digital work is valid by using the record signature data, the calculation digest values, and the remaining record digest values” of Claim 1, it is not clear how to use the record signature data, calculation digest values and remaining digest values in order to verify whether the digital work recorded on the recording medium is valid.

(3) Regarding the description “the signature verifying unit verifies validity of the digital work by calculating one or more secondary calculation digest values based on the calculation digest values and the remaining record digest values, and performing a digital signature verification with use of the record signature data, the plurality of secondary record digest values, and the secondary calculation digest values” of Claim 2,

it is not clear

1) how the signature verifying unit obtains the “secondary calculation digest values” from the recording medium; and

2) how the record signature data, the secondary record digest values and secondary calculation digest values are used to perform the digital signature verification.

(4) Regarding the description “using unit operable to use the digital work” of Claim 8 and the description “using unit operable to use the digital work recorded on the recording medium” of Claim 1, the relationship of these two is not clear.

(5) Regarding the “data processing program” and the “control program” of Claim 15, the relationship of these two is not clear.

(6) Regarding the “data processing program” and the “control program” of Claim 16, the relationship of these two is not clear.

(7) Regarding the description “the data processing program to be transmitted and received via telecommunications” of Claim 16, it is not clear that from which apparatus to which apparatus the data processing program is transmitted and received via telecommunications.

<Claims in which no bases for rejection are found>

As to the invention related to Claims 3-7, 9, 10 and 12, no bases for rejection are found at this time. If a basis for rejection is newly found, an office action will be issued.

#### List of Cited References

1. Japanese Laid-Open Patent Application S63-225840
2. Japanese Laid-Open Patent Application H3-151738
3. Japanese Laid-Open Patent Application 2001-142398

#### Record of Search Results on Prior Art Reference(s)

- Field of Search IPC H04L 9/32  
G09C 1/00

- Prior Art Reference

Japanese Laid-Open Patent Application 2006-33729

Japanese Laid-Open Patent Application 2005-94146

Japanese Laid-Open Patent Application 2003-318887

Japanese Laid-Open Patent Application 2001-265217

WO Publication International Phase 01/082267

The Record of Search Results on Prior Art Reference(s) is not a component of the Notification of Reasons for Refusal.

If you have any inquiry regarding this office action or request for a meeting, please call me at the following numbers.

Nobuyuki Ishida

Information Security

Fourth Patent Examination Department

TEL. 03(3581)1101 Extension 3546

FAX. 03(3501)0737

## 拒絶理由通知書

特許出願の番号 特願2006-519466  
起案日 平成19年10月19日  
特許庁審査官 石田 信行 9469 5S00  
特許出願人代理人 中島 司朗 様  
適用条文 第29条柱書、第29条第2項、第36条

この出願は、次の理由によって拒絶をすべきものです。これについて意見がありましたら、この通知書の発送の日から60日以内に意見書を提出してください。

## 理 由

1. この出願の下記の請求項に係る発明は、その出願前に日本国内又は外国において、頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第29条第2項の規定により特許を受けることができない。
2. この出願の下記の請求項に係る発明は、下記の点で特許法第29条第1項柱書に規定する要件を満たしていないので、特許を受けることができない。
3. この出願は、特許請求の範囲の記載が下記の点で、特許法第36条第6項第2号に規定する要件を満たしていない。

記 (引用文献等については引用文献等一覧参照)

- ・理由1
- ・請求項: 11
- ・引用文献等: 1～3

## [ 備考 ]

引用文献1 (【特許請求の範囲】、第2頁左下欄第12行～第3頁右上欄第9行参照)、引用文献2 (第1～8図参照) 及び引用文献3 (第1～4, 11, 12図参照) には、デジタル著作物(メッセージ、ファイル、複数のデジタル文書)を構成する複数のデータブロック(ブロック、分割したメッセージ、デジタル文書)から生成された複数の記録要約値(個別のMAC、圧縮文H(i)、ダイジェスト)と、前記記録要約値群に基づいて生成された記録署名データ(グローバルMAC、検証用データH、統合ダイジェスト)とを生成する情報記録方式が記載されている。



## ・理由2

## [備考]

(A) 請求項11に係る発明は、記録媒体に記憶される、複数のデータブロックから生成された複数の記録要約値、及び、記録要約値群に基づいて生成された記録署名データにのみ特徴を有するものであり、情報の単なる提示であって、自然法則利用の技術的手段を用いているとは認められないことから、特許法第29条第1項柱書の要件を備えていない。

(B) 特許請求の範囲に記載された発明は、以下の点において、データ処理装置のどのハードウェア資源を用いて情報処理を行うのかを特定していないことから、自然法則利用の技術的手段を用いていないものであり、特許法第29条第1項柱書の要件を備えていない。

(1) 請求項13の「前記記録媒体に記録されている前記デジタル著作物を利用する利用ステップ、前記データブロックからランダムに所定数個の選択データブロックを選択する選択ステップ、・・・・・・・・・・ 前記検証の結果、不正であると判断される場合に、前記デジタル著作物の利用を停止する利用制御ステップ」の記載は、データ処理装置のどのハードウェア資源を用いて、1) 記録媒体に記録されているデジタル著作物を利用するのか、2) 所定数個の選択データブロックを選択するのか、3) 各選択データブロックから演算要約値を算出するのか、4) 選択データブロックを除く他のデータブロックに対応する残存要約値を読み出すのか、5) 記録媒体に記録されているデジタル著作物の正当性を検証するのか、を特定していないことから、ハードウェア資源を用いて具体的に実現されているものとは認められない。

(例えば、データ処理装置の利用手段、選択手段、演算手段、読出手段、署名検証手段、利用制御手段、などのハードウェア資源を用いていることを明確に記載することを検討して下さい。(2) 以下においても同様。)

(2) 請求項14の「前記記録媒体に記録されている前記デジタル著作物を利用する利用ステップと、前記データブロックからランダムに所定数個の選択データブロックを選択する選択ステップと、・・・・・・・・・・ 前記検証の結果、不正であると判断される場合に、前記デジタル著作物の利用を停止する利用制御ステップ」の記載は、データ処理装置のどのハードウェア資源を用いて、1) 記録媒体に記録されているデジタル著作物を利用するのか、2) 所定数個の選択データブロックを選択するのか、3) 各選択データブロックから演算要約値を算出するのか、4) 選択データブロックを除く他のデータブロックに対応する残存要約値を読み出すのか、5) 記録媒体に記録されているデジタル著作物の正

当性を検証するのか、を特定していないことから、ハードウェア資源を用いて具体的に実現されているものとは認められない。

・理由3

[ 備考 ]

特許請求の範囲に記載された発明の構成要素又は各々の構成要素間の関係が、以下の点において不明確である。

(1) 請求項1, 13, 14の「前記記録媒体に記録されている前記デジタル著作物を利用する利用手段(利用ステップ)」において、デジタル著作物を利用するとは、具体的にどのようなことを意味しているのか不明確である。

(2) 請求項1の「記録媒体に記録されている前記記録署名データ、前記演算要約値及び前記残存要約値を用いて、前記記録媒体に記録されている前記デジタル著作物の正当性を検証する署名検証手段」において、記録署名データ、演算要約値及び残存要約値をどのように用いて、デジタル著作物の正当性を検証しているのか不明確である。

(3) 請求項2の「前記署名検証手段は、前記演算要約値及び前記残存要約値に基づいて、1個以上の二次演算要約値を算出し、前記記録署名データ、前記二次記録要約値及び前記二次演算要約値を用いて、デジタル署名検証を施して、前記デジタル著作物の正当性を検証する」において、

1) 署名検証手段は「二次記録要約値」を、記録媒体からどのようにして取得しているのか不明確である。

2) 記録署名データ、二次記録要約値及び二次演算要約値をどのように用いて、デジタル署名検証を行っているのか不明確である。

(4) 請求項8の「前記デジタル著作物を利用する利用手段」と、請求項1の「前記記録媒体に記録されている前記デジタル著作物を利用する利用手段」とは、どのような関係にあるのか不明確である。

(5) 請求項15の「データ処理プログラム」と「制御プログラム」とは、どのような関係にあるのか不明確である。

(6) 請求項16の「データ処理プログラム」と「制御プログラム」とは、どのような関係にあるのか不明確である。

(7) 請求項16の「データ処理プログラムは、電気通信回線を通じて送受信さ

れる」において、データ処理プログラムは、どの装置からどの装置へ電気通信回線を通じて送受信されているのか不明確である。

### ＜拒絶の理由を発見しない請求項＞

請求項 3 ～ 7, 9, 10, 12 に係る発明については、現時点では、拒絶の理由を発見しない。拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

## 引用文献等一覽

1. 特開昭63-225840号公報
2. 特開平3-151738号公報
3. 特開2001-142398号公報

## 先行技術文献調査結果の記録

・調査した分野      I P C          H 0 4 L    9 / 3 2  
   G 0 9 C    1 / 0 0

・先行技術文献 特開2006-33729号公報  
特開2005-94146号公報  
特開2003-318887号公報  
特開2001-265217号公報  
国際公開第01/082267号

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。

この拒絶理由通知の内容に関するお問い合わせ、または面接のご希望がございましたら下記までご連絡下さい。

特許審査第四部 情報セキュリティ 石田 信行  
TEL. 03 (3581) 1101 内線3546  
FAX. 03 (3501) 0737